ATTACHMENT B

ITEMS TO BE SEIZED

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 18 U.S.C. § 2252A (possession and receipt of child pornography), including:

A. The following topics:

1. Child pornography;

2. The sexual abuse or exploitation of children;

3. Child erotica;

4. The identity of any child depicted in videos and photographs located in the equipment or discussed in any communications related to child pornography or the sexual abuse or exploitation of children;

5. Internet activity reflecting a sexual interest in minors or child pornography;

6. Freenet;

7. Membership in online groups, clubs, or services that provide, make accessible, or otherwise concern child pornography.

B. Any communication(s) relating to child pornography, the sexual abuse or exploitation of children, or the identity of any child depicted in videos and photographs located in the equipment;

C. Any social media account(s) or communication application(s) used to send or receive any communication(s) relating to child pornography, the sexual abuse or exploitation of children, or the identity of any child depicted in videos and photographs located in the equipment;

D. The identity, location, and travel of any co-conspirators, as well as any co-

conspirators' acts taken in furtherance of the crimes listed above;

E. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):

1. evidence of who used, owned, or controlled the computer equipment;

2. evidence of computer software that would allow others to control the items, evidence of the lack of such malicious software, and evidence of the presence or absence of security software designed to detect malicious software;

3. evidence of the attachment of other computer hardware or storage media;

4. evidence of counter forensic programs and associated data that are designed to eliminate data;

5. evidence indicating how and when the computer equipment was accessed or used;

6. records of or information about any Internet Protocol addresses used;

7. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;

8. records and tangible objects pertaining to accounts held with companies providing internet access or remote storage of either data or storage media;

9. records of or information about the computer equipment's internet activity; and

10. contextual information necessary to understand the evidence described in this attachment.

F. Records and tangible objects relating to the ownership, occupancy, or use of the SUBJECT PREMISES (such as utility bills, phone bills, rent payments, mortgage payments, photographs, insurance documentation, receipts and check registers); and

G. Records, information, and items relating to the ownership or use of computer equipment found in the SUBJECT PREMISES or on the person of the Subject, including sales receipts, bills for Internet access, and handwritten notes.

II. All computer hardware, computer software, computer-related documentation, and storage media. Off-site searching of these items shall be limited to searching for the items described in Paragraph I.

DEFINITIONS

For the purpose of this warrant:

A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.

B. "Computer hardware" means any electronic device capable of data processing (such as a computer, smartphone, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device (such as electronic data security hardware and physical locks and keys).

C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Computer related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

G. A "record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

H. "Child Pornography," as defined in 18 U.S.C. § 2256(8)(A), means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

I. "Child Erotica" means materials or items that are sexually arousing to persons

having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions; this also includes texts or discussions regarding minors engaged in sexual acts or conduct.

EXECUTION

Searching agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence authorized by this warrant, as outlined above. If, however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

RETURN OF SEIZED COMPUTER EQUIPMENT

If the owner of the seized computer equipment requests that it be returned, the government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the government determines that some or all of this equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If the computer equipment contains contraband, it will not be returned. If the computer equipment cannot be returned, agents will attempt to make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do

not contain or constitute contraband; passwords, account information, or personally-identifying information of victims; or the fruits or instrumentalities of crime.